IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A computer program product operable to control a computer to issue an alert for an out-of-date update status of a malware scanner, said computer program product comprising:

(i) reading logic operable to read an update status field associated with a computer file to be scanned by a current malware scanner, said update status field being indicative of an update status of a previous malware scanner that has scanned said computer file and associated said update status field with said computer file;

(ii) comparison logic operable to compare said update status of said previous malware scanner with an update status of said current malware scanner;

(iii) alert issuing logic operable if said update status of said current malware scanner does not match said update status of said previous malware scanner to issue an update status alert indicative of an out-of-date update status for whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status;

(iv) change logging logic operable to log changes to said update status field to create a change history in an update status tracking database to enable identification of weaknesses within update status management based on the change history;

wherein, if said current malware scanner has a less out-of-date update status than said previous malware scanner, then said update status field associated with said computer file is changed to correspond to said current malware scanner;

wherein said update status alert includes one or more of:

(i) a user alert issued on whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status; and

(ii) an administrator alert issued to an administrator of whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status;

wherein, if there is no said update status associated with said computer file at a first malware scanning, then said update status field is generated and associated with said computer file, and said update status tracking database is updated.

2. (Original) A computer program product as claimed in claim 1, wherein said update status field is included as a property field within said computer file.

3. (Original) A computer program product as claimed in claim 1, wherein said update status field is included within an update status file passed together and associated with said computer file between malware scanners.

4. (Original) A computer program product as claimed in claim 3, wherein said update status file and said computer file are combined into a combined file that is passed as a single entity between malware scanners.

5. (Original) A computer program product as claimed in claim 4, wherein said combined file is a file compressed combination of said update status file and said computer file.

6. (Cancelled)

7. (Cancelled)

8. (Cancelled)

9. (Original) A computer program product as claimed in claim 1, wherein said computer file is an e-mail attachment.

10. (Original) A computer program product as claimed in claim 1, wherein said current malware scanner and said previous malware scanner are part of a tiered malware scanner.

11. (Original) A computer program product as claimed in claim 1, wherein said update status field includes one or more of:

(i) a malware scanner computer program product identifier;

(ii) a computer hardware identifier;

(iii) a scanner engine program version identifier; and

(iv) a malware definition data version identifier.

12. (Previously Presented) A computer program product as claimed in claim 1, wherein said malware scanner serves to detect one or more of:

(i) a computer virus;

(ii) a Trojan computer program;

(iii) a worm computer program;

(iv) a banned computer program; and

(v) banned content within a e-mail.

13. (Currently Amended) A method of alerting an out-of-date update status of a malware scanner, said method comprising the steps of:

(i) reading an update status field associated with a computer file to be scanned by a current malware scanner, said update status field being indicative of an update status of a previous malware scanner that has scanned said computer file and associated said update status field with said computer file;

(ii) comparing said update status of said previous malware scanner with an update status of said current malware scanner;

(iii) if said update status of said current malware scanner does not match said update status of said previous malware scanner, then issuing an update status alert indicative of an out-of-date update status for whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status; and

(iv) logging changes to said update status field to create a change history in an update status tracking database to enable identification of weaknesses within update status management based on the change history;

wherein, if said current malware scanner has a less out-of-date update status than said previous malware scanner, then said update status field associated with said computer file is changed to correspond to said current malware scanner;

wherein said update status alert includes one or more of:

(i) a user alert issued on whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status; and

(ii) an administrator alert issued to an administrator of whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status;

wherein, if there is no said update status associated with said computer file at a first malware scanning, then said update status field is generated and associated with said computer file, and said update status tracking database is updated.

14. (Original) A method as claimed in claim 13, wherein said update status field is included as a property field within said computer file.

15. (Original) A method as claimed in claim1, wherein said update status field is included within an update status file passed together and associated with said computer file between malware scanners.

16. (Original) A method as claimed in claim 15, wherein said update status file and said computer file are combined into a combined file that is passed as a single entity between malware scanners.

17. (Original) A method as claimed in claim 16, wherein said combined file is a file compressed combination of said update status file and said computer file.

18. (Cancelled)

19. (Cancelled)

20. (Cancelled)

21. (Original) A method as claimed in claim 13, wherein said computer file is an e-mail attachment.

22. (Original) A method as claimed in claim 13, wherein said current malware scanner and said previous malware scanner are part of a tiered malware scanner.

23. (Original) A method as claimed in claim 13, wherein said update status field includes one or more of:

(i) a malware scanner computer program product identifier;

(ii) a computer hardware identifier;

(iii) a scanner engine program version identifier; and

(iv) a malware definition data version identifier.

24. (Previously Presented) A method as claimed in claim 13, wherein said malware scanner serves to detect one or more of:

(i) a computer virus;

(ii) a Trojan computer program;

(iii) a worm computer program;

(iv) a banned computer program; and

(v) banned content within a e-mail.

25. (Currently Amended) Apparatus for issuing an alert for an out-of-date update status of a malware scanner, said apparatus comprising:

(i) a reader operable to read an update status field associated with a computer file to be scanned by a current malware scanner, said update status field being indicative of an update status of a previous malware scanner that has scanned said computer file and associated said update status field with said computer file;

(ii) a comparitor operable to compare said update status of said previous malware scanner with an update status of said current malware scanner;

(iii) an alert issuer operable if said update status of said current malware scanner does not match said update status of said previous malware scanner to issue an update status alert indicative of an out-of-date update status for whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status; and

(iv) a change logger operable to log changes to said update status field to create a change history in an update status tracking database to enable identification of weaknesses within update status management based on the change history;

wherein, if said current malware scanner has a less out-of-date update status than said previous malware scanner, then said update status field associated with said computer file is changed to correspond to said current malware scanner;

wherein said update status alert includes one or more of:

(i) a user alert issued on whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status; and

(ii) an administrator alert issued to an administrator of whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status;

wherein, if there is no said update status associated with said computer file at a first malware scanning, then said update status field is generated and associated with said computer file, and said update status tracking database is updated.

26. (Original) Apparatus as claimed in claim 25, wherein said update status field is included as a property field within said computer file.

27. (Original) Apparatus as claimed in claim 25, wherein said update status field is included within an update status file passed together and associated with said computer file between malware scanners.

28. (Original) Apparatus as claimed in claim 27, wherein said update status file and said computer file are combined into a combined file that is passed as a single entity between malware scanners.

29. (Original) Apparatus as claimed in claim 28, wherein said combined file is a file compressed combination of said update status file and said computer file.

30. (Cancelled)

31. (Cancelled)

32. (Cancelled)

33. (Original) Apparatus as claimed in claim 25, wherein said computer file is an e-mail attachment.

34. (Original) Apparatus as claimed in claim 25, wherein said current malware scanner and said previous malware scanner are part of a tiered malware scanner.

35. (Original) Apparatus as claimed in claim 25, wherein said update status field includes one or more of:

(i) a malware scanner computer program product identifier;

(ii) a computer hardware identifier;

(iii) a scanner engine program version identifier; and

(iv) a malware definition data version identifier.

36. (Previously Presented) Apparatus as claimed in claim 25, wherein said malware scanner serves to detect one or more of:

(i) a computer virus;

(ii) a Trojan computer program;

(iii) a worm computer program;

(iv) a banned computer program; and

(v) banned content within a e-mail.

37. (New) A computer program product as claimed in claim 1, wherein said update status alert triggers an automatic update to said malware scanner in accordance with one of administrator preferences and user preferences.